REMARKS/ARGUMENTS

In this Amendment After Final Under 37 C.F.R. § 1.116 ("Amendment After Final"), Applicant proposes to amend claim 8 to recite, inter alia, "[a]n accumulator for accelerating speed of a Montgomery modular multiplier, for reducing power consumption of a Montgomery modular multiplier, or for accelerating the speed of and reducing the power consumption of a Montgomery modular multiplier in a cryptosystem"; to amend claim 20 to recite, inter alia, "wherein the compressors of the first group are a first compressor, respectively"; to amend claim 22 to recite, inter alia, "wherein the compressors of the second group are a second compressor, respectively"; to amend claim 25 to recite, inter alia, "wherein the first compressors include three full adders"; to amend claim 26 to recite, inter alia, "wherein the second compressors include one half adder and two full adders"; and amend claim 51 to recite, inter alia, "[a] method of accumulating for accelerating speed of a Montgomery modular multiplier, for reducing power consumption of a Montgomery modular multiplier, or for accelerating the speed of and reducing the power consumption of a Montgomery modular multiplier in a cryptosystem"; all in order to better define the claimed invention. No new matter is introduced.

Applicant makes no amendments in response to the rejections under 35 U.S.C. § 103(a).

Prior to entry of the Amendment After Final, claims 1-61 were pending in the application. After entry of the Amendment After Final, claims 1-61 remain pending in the application.

In the Office Action, the Examiner rejected claims 20 and 22 under 35 U.S.C. § 112, ¶ 2; rejected claims 8-41 and 51-55 under 35 U.S.C. § 101; rejected claims 8-17, 23, 27, and 51-54 under 35 U.S.C. § 103(a) as being unpatentable over "New VLSI Architecture of RSA Public-Key Cryptosystem" by Wang et al. ("Wang"); and rejected claims 19-22, 25, and 26 under 35 U.S.C. § 103(a) as being unpatentable over Wang in view of U.S. Patent No. 5,796,645 to Peh et al. ("Peh").

Applicant respectfully traverses the Examiner's rejections under 35 U.S.C. § 103(a).

Claims 1-7, 42-50, and 56-61

Regarding withdrawn claims 1-7, 42-50, and 56-61, Applicant notes that MPEP 821.01 states in relevant part (emphasis added):

> If the requirement is repeated and made final, in that and in each subsequent action, the claims to the non-elected invention should be treated by using form paragraph 8.05.

And form paragraph 8.05 states:

> Claim **[1]** withdrawn from further consideration pursuant to 37 CFR 1.142(b), as being drawn to a nonelected **[2]**, there being no allowable generic or linking claim. Applicant timely traversed the restriction (election) requirement in the reply filed on **[3]**.

Applicant is unable to find the complete form paragraph 8.05 in the Office Action mailed on October 15, 2007. Applicant is similarly unable to find the form paragraph 8.05 in the Final Office Action.

Claim Rejection Under 35 U.S.C. § 112, ¶ 2

As discussed above, Applicant proposes to amend claim 20 to recite, inter alia, "wherein the compressors of the first group are a first compressor, respectively" and to amend claim 22 to recite, inter alia, "wherein the compressors of the second group are a second compressor, respectively".

Applicant submits that these amendments obviate the rejection of claims 20 and 22 under 35 U.S.C. § 112, ¶ 2.

Claim Rejection Under 35 U.S.C. § 101

As discussed above, Applicant proposes to amend claim 8 to recite, inter alia, "[a]n accumulator for accelerating speed of a Montgomery modular multiplier, for reducing power consumption of a Montgomery modular multiplier, or for accelerating the speed of and reducing the power consumption of a Montgomery modular multiplier in a cryptosystem" and to amend claim 51 to recite, inter alia, "[a] method of accumulating for accelerating speed of a Montgomery modular multiplier, for reducing power consumption of a Montgomery modular multiplier, or for accelerating the speed of and reducing the power consumption of a Montgomery modular multiplier in a cryptosystem".

Applicant submits that independent claims 8 and 51, at least as amended, accomplish a practical application (and, thus, so do dependent claims 9-41 and 52-55); that the practical application yields a real-world result that is useful, tangible, and concrete; that neither the accumulators of claims 8-41 nor the methods of claims 51-55 cover every substantial practical application; and that because the accumulators of claims 8-41 and the methods of claims 51-55 are implemented in associated cryptosystems, they do not preempt use of the underlying algorithm. As a result, Applicant submits that these amendments obviate the rejection of claims 8-41 and 51-55 under 35 U.S.C. § 101.

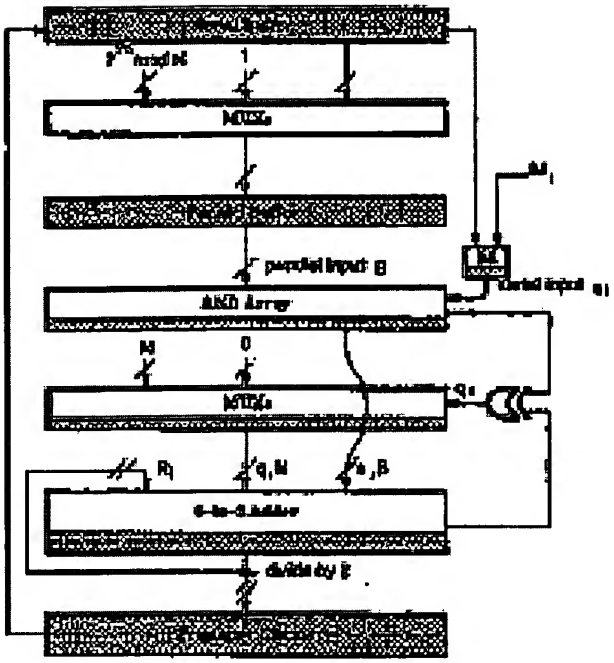
Wang

Applicant submits that FIG. 2 of Wang (depicted below) shows implementation of the Montgomery Algorithm for Modular Multiplication (Radix 2) discussed in Section 2.2 of Wang. That algorithm involves the following two equations:

$$q_i = R_i + a_i B \pmod 2; \text{ and}$$

$$R_{i+1} = (R_i + a_i B + q_i N)/2.$$

Applicant submits that in FIG. 2, the first equation is implemented in the input to the MUXs on the right-hand side of the MUXs and the second equation is implemented in the 4-to-2 Adder.

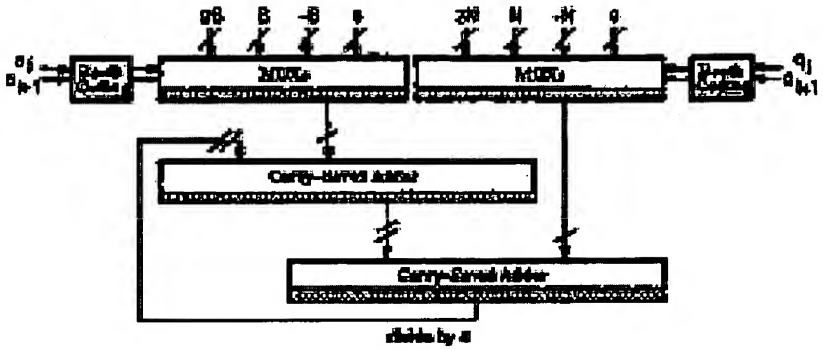


Applicant submits that FIG. 5 of Wang (depicted below) shows implementation of the Interleaving Method discussed in Section 4.1 of Wang. That algorithm involves the following two equations:

$$q_{i+1} = R_{i+1} + a_{i+1}B \pmod 2; \text{ and}$$

$$R_{i+2} = [R_i + (2a_{i+1} + a_i)B + (2q_{i+1} + q_i)N]/4.$$

Applicant submits that in contrast to FIG. 2, FIG. 5 does not show implementation of the first equation. Instead, Applicant submits that FIG. 5 essentially shows implementation of only the second equation.



Applicant submits that FIG. 5 of Wang shows two Carry-Saved Adders, the first one (CSA1) higher and to the left, the second one (CSA2) lower and to the right. Applicant also submits that CSA1 shows implementation of only a first portion of the second equation (i.e., the inputs to CSA1 are R_i and $(2a_{i+1} + a_i)B$ and the output of CSA1 is the partial sum $R_i + (2a_{i+1} + a_i)B$), while CSA2 shows implementation of a second portion of the second equation (i.e., the inputs to CSA2 are the partial sum $R_i + (2a_{i+1} + a_i)B$ and $(2q_{i+1} + q_i)N$) and the output of CSA2 is the partial sum $R_i + (2a_{i+1} + a_i)B + (2q_{i+1} + q_i)N$, that divided by 4 is R_{i+2}).

As a result, Applicant submits that the input to CSA2 from CSA1 is the partial sum $R_i + (2a_{i+1} + a_i)B$. Similarly, the input to CSA1 from CSA2 is the running total R_{i+2}.

Claim Rejections Under 35 U.S.C. § 103(a)

Applicant submits that the Examiner has failed to establish a proper prima facie case of obviousness for at least the following reasons.

Assuming, arguendo, that CSA1 includes a plurality of compressors, each of those compressors does not receive at least a multiple modulus q_xN, as recited in claim 8, because—as discussed above—the inputs to CSA1 are R_i (or R_{i+2}) and $(2a_{i+1} + a_i)B$. Similarly, assuming, arguendo, that CSA2 includes a plurality of compressors, each of those compressors does not receive at least a partial product a_xB, as also recited in claim 8, because—as discussed above—the inputs to CSA2 are the partial sum $R_i + (2a_{i+1} + a_i)B$ and $(2q_{i+1} + q_i)N$.

As also discussed above, neither the input to CSA1 nor the input to CSA2 includes "a corresponding current sum . . . and a corresponding current carry", as recited in claim 8. Similarly, neither CSA1 nor CSA2 is "adapted to produce a corresponding next sum and a corresponding next carry", as also recited in claim 8.

Additionally, FIG. 5 of Wang does not disclose "receiving a plurality of . . . corresponding current sums . . . and corresponding current carries to produce a corresponding next sum and next carry", as recited in claim 51.

Thus, contrary to the allegations of the Office Action (p. 3, ¶ 5), Wang does not disclose at least "an accumulator including a carry save adder inherently having a plurality of compressors . . . each of the plurality of compressors receiving a multiple modulus (a multiple of N from MUXs), a partial product (a multiple of B from MUXs)" (emphases added).

Additionally, contrary to the allegations of the Office Action (pp. 3-4, ¶ 5), Wang does not disclose at least "an accumulator including a carry save adder

inherently having a plurality of compressors . . . each of the plurality of compressors receiving . . . a corresponding current sum and a corresponding current carry (the feedback from the [unidentified] carry save adder), and producing a corresponding next sum and a corresponding next carry (the output from the [unidentified] carry save adder)" (emphases added).

Applicant notes that the Examiner does not argue that Peh overcomes these deficiencies of Wang.

As a result, Applicant submits that independent claims 8 and 51 are patentable under 35 U.S.C. § 103(a) over Wang and over any proper combination of Wang, Peh, and the other art of record. Applicant further submits that dependent claims 9-41 and 52-55 are patentable under 35 U.S.C. § 103(a) over Wang and over any proper combination of Wang, Peh, and the other art of record, at least for the same reasons that claims 8 and 51 are patentable, from which claims 9-41 and 52-55 directly or indirectly depend.

Request for Reconsideration and Allowance

Accordingly, in view of the above amendments and remarks, reconsideration of the rejections and allowance of each of claims 1-61 in connection with the present application is earnestly solicited.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

If necessary, the Director of the U.S. Patent and Trademark Office is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; in particular, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By _____

John A. Castellano, Reg. No. 35,094

P.O. Box 8910
Reston, VA 20195
703.668.8000

JAC/LFG:hcw